OFFICE OF THE STATE CHIEF INFORMATION OFFICER

Teri Takai
California Chief Information Officer

September 23, 2010

Federal Communications Commission
455 12th Street, S.W.
Washington, D.C. 20554

Subject: State of California, Office of the State Chief Information Officer Response to FCC Request for Comment on NBP Recommendation to Create Cybersecurity Roadmap: PS Docket No. 10-146; GN Docket No. 09-51

Dear Sir/Madam:

The California Office of the State Chief Information Officer (OCIO) appreciates the opportunity to comment on the Federal Communications Commission (FCC) proposal to create a cybersecurity roadmap to identify vulnerabilities and plans to address vulnerabilities to communications networks and end-users.

What are the most vital cyber security vulnerabilities for communications networks or users?

In the case of public safety, any cyber security threats that put the lives of citizens or emergency responders at stake are consider the most vital. The FCC cybersecurity roadmap should address issues that pose a threat to the confidentiality, integrity or availability (CIA) of the information and interconnected systems upon which essential public services rely. This includes all interconnected information systems, communication networks and their underlying infrastructure.

The Internet and its infrastructure were not designed with security in mind; yet it now serves as the basis of many essential public services. The National Broadband Plan (NBP) proposes continued expansion of wireless and IP-based communications use as the foundation of all future communications.

It's important to recognize that threats of disasters and disruptions before voice over Internet Protocol (VoIP) in the telecommunications sector have long included people, equipment, natural disasters, software, hardware and environmental factors. The threats in each of these areas will still exist, but increase exponentially in some areas with a move

to expanded wireless and IP-based infrastructure and use. For purpose of this response, we will focus on the areas of people, physical infrastructure, software, hardware and environmental factors.

People – Inadvertent configuration errors and unauthorized entry into communication networks with intent to disrupt, exploit, or sabotage can severely affect preparedness and response. With increased reliance on IP-based services even an inadvertent configuration error by an unqualified technician could potentially have devastating consequences. Further, the disgruntled employee with intimate knowledge about core or critical infrastructure can cause severe damage or disruption. California experienced a recent example of this when the fiber-optic cables of AT&T in the heart of its Silicon Valley were cut; it led to a significant 17-hour and cascading outage and service disruption for AT&T's public-safety 911 and financial sector customers, as well as other co-located providers and their customers.

Physical Infrastructure – Core and critical infrastructure assets are easily accessible (e.g., via manholes) and often lack the ability to attribute malicious acts to a particular actor with any certainty.

Software/ Hardware – Software and hardware which has not been developed with security in mind and which has not undergone rigorous testing before being pushed to production often contain vulnerabilities. Vulnerabilities, once discovered or known, can and often are exploited very easily. Exploits can take the form of breaches in confidentiality (intercepting, eavesdropping, and recording of communications), breaches of data integrity (data manipulation), and availability (e.g., outage, denial of service, other disruption).

Known vulnerabilities are identified in the thousands per-day. As an example, the United States Computer Emergency Readiness Team (US-CERT) publishes information about a wide variety of vulnerabilities at: http://www.kb.cert.org/vuls

Environmental Factors – The Internet is now viewed as a critical asset that may be the subject of the next large-scale targeted attack against the U.S. Cyberspace has become the fifth domain of warfare, after land, sea, air and space. Because the Internet was not designed with security in mind and because much of our essential consumer and public services are now IP-based, we are more vulnerable to such an attack. Such an attack may be a trivial matter for the attacker, yet yield devastating economic consequences for us in the U.S.
As examples we point to the 2000 Distributed Denial of Service (DDoS) attack, a 15-year old boy in Montreal launched against Yahoo, E-Trade, eBay and CNN 2007 Denial of Service; and the 2009 DoS attack against the Estonian government.

How can these vulnerabilities be addressed?
The FCC and the NBP offer ways in which some of the vulnerabilities may be addressed, such as a market incentive-voluntary certification program for service providers. While we agree with that approach, we also offer the following recommendations:

1. Ensure cybersecurity requirements (confidentiality, integrity and availability) are addressed in the initial communications system design phase - not after implementation.

2. Develop strong access control systems to protect core and critical infrastructure (including manhole access).

3. Develop a strong and streamlined credentialing process for those with authorized access to core and critical infrastructure and authorized users on a public safety network. Ensure employees are both qualified and have undergone fingerprinting and a criminal background check.

4. Participate and create incentives for providers to educate end-users about cybersecurity risks and steps that they can take to protect themselves.

What role should the Commission play in addressing them?
The role of addressing cyber security assumes the Commission takes on the responsibility of prevention and protection. This is a dynamic environment that evolves quickly and requires strategies that can focus on deploying effective and efficient controls quickly.

However, the role of addressing vulnerabilities is a shared responsibility of government, industry and end-users. Placing the responsibility on a single entity may result in vulnerabilities that go undetected and continued cyber attacks. The Commission can best serve in an advisory role, with enforcement, coordination, and management delegated to entities that are familiar with implementing cyber security measures. The Commission should play a role in educating consumers on risk and best practices, and can advise all broadband network providers to design their systems with cybersecurity risk mitigation measures.

We recommend the Commission consider the following:

1. Facilitate the adoption and implementation of interoperability and security standards for wireless and IP-based communications where currently lacking (e.g., VoIP products).

2. Support a voluntary or mandatory product accreditation process where the products undergo a rigorous testing process for compliance with adopted interoperability and security standards.

3. Support the maintenance and enforcement of a unified command in emergency response.

4. Facilitate the identification of interconnections and disaster recovery prioritization in national disasters has been addressed before a disaster strikes.

If the Commission does not play a role in addressing these vulnerabilities and problems, what agency or entity would fulfill that role?

Again the problem is a shared responsibility and all sectors must participate in its address. Information sharing is critical to an effective response to cyber security threats and creating a new entity may only complicate how that information is disseminated. Reluctance to share information exists at various government and private levels due to cultural and legal constraints. For this reason, existing agencies like the Department of Homeland Security's (DHS) National Cyber Security Division (NCSD) may better fit the role of addressing cyber vulnerabilities from a National protection perspective, as they currently manage security for the government IT infrastructure and coordinate cyber security efforts with the state and local government jurisdictions and the private sector.

The Commission should work in tandem with others within the Federal government to ensure its cybersecurity roadmap is aligned with other cybersecurity plans and initiatives currently under development, such as the National Infrastructure Protection Plan, the National Cyber Incident Response Plan and the Comprehensive National Cybersecurity Initiative. It is important that these interdependent plans present a unified approach and response to addressing cybersecurity threats and that private and public sectors at the state and local levels are on board.

How should the Commission coordinate its efforts with other agencies of government?

In an advisory position, the Commission can provide support to the government's cyber security initiatives and polices. This role should also include proactively engaging its constituents for risk mitigation suggestions as it has done through this process.

Sincerely,

Teri Takai
State Chief Information Officer